ESET MSP PROGRAM

6 CONSEILS POUR UNE OFFRE MSP EFFICACE

En tant que partenaire MSP, il est de votre devoir d'assurer une expertise optimale en cybersécurité, d'offrir un panel de solutions de sécurité et de services adaptés et de délivrer une réelle valeur ajoutée à vos clients.

1 Qui est votre client ?

Une collaboration réussie est construite sur la confiance. Afin de créer une atmosphère positive, vous pouvez par exemple proposer un audit de sécurité classique sur les systèmes informatiques de vos clients. Cela permettra d'affirmer votre expertise tout en soulevant d'éventuelles menaces qui pourraient ensuite déboucher sur l'ajustement d'une stratégie de sécurité personnalisée de votre client, ou en la créant de toutes pièces.

Cette liste n'est pas exhaustive mais ces éléments permettent de mettre en lumière des besoins différents et propres à chaque secteur/industrie. Par exemple, dans le monde agricole, l'informatique peut être vu comme un "mal nécessaire" qui doit simplement se contenter de fonctionner. A l'inverse, un client opérant dans le milieu de la santé fonctionnera probablement à l'aide d'un business model basé sur la collecte et l'analyse de données sensibles relatives à ses patients. Sur ce cas précis, le chiffrement et les technologies liées à la protection des données sont incontournables.

Grâce à l'enquête préalable, vous pourrez identifier le modèle de sécurité approprié à votre client et **l'aider à définir le kit de défense adapté** qui lui permettra d'améliorer son niveau de protection.

Ladite évaluation devra vous apporter des éléments concrets de réponses à certaines questions, parmi les suivantes (entre autres considérations) :

1. Au sein de quelle **verticale** le client opère-t-il et quelles sont les spécificités de cette dernière ?
2. **De quelle manière et pourquoi** le client a-t-il recours à un système informatique ?
3. **Qu'est-ce qui est stocké** par le client sur ce(s) système(s) ?
4. **Les appareils du client** sont-ils utilisés uniquement sur site ou également à distance ?
5. Quels **types d'utilisateurs** sont connectés au réseau ?
6. Quels **problèmes informatiques** le client a-t-il connus par le passé ?

2 Appliquez une politique de cyber-hygiène

En tant que spécialiste de la sécurité, vos propres systèmes doivent servir d'exemples à vos clients. Il vous faut donc suivre les meilleures règles de cyber-hygiène pour vos réseaux et dispositifs pour ensuite pouvoir les appliquer à l'infrastructure informatique de vos clients. C'est en appliquant une bonne gestion des correctifs, en mettant à jour vos systèmes d'exploitation, applications et solutions de sécurité, que vous éviterez de nombreuses vulnérabilités potentielles.

Vous pouvez considérablement réduire l'ampleur des attaques et empêcher la création de nouvelles failles de sécurité en administrant les droits d'accès pour le compte de votre client lors de l'installation de nouveaux logiciels. Une approche similaire devrait également être de mise même lorsque des clients souhaitent que leur département informatique s'occupe des solutions de sécurité et des logiciels.

L'importance d'une bonne hygiène en cybersécurité est particulièrement parlante avec l'exemple de l'incident de 2017, mieux connu sous le nom de Wanna-Cryptor.D (ou WannaCry). Bien que la vulnérabilité sous Windows ait été détectée et réparée à l'aide d'un correctif des mois avant l'attaque, des centaines de milliers de postes n'ont pas effectué la correction (dont beaucoup issus de PME).

Mettez de l'ordre dans vos pratiques informatiques

1. Réduisez la surface d'attaque en désactivant ou en désinstallant les services et logiciels qui ne sont pas nécessaires
2. Effectuez une analyse des réseaux en vue de détecter les comptes à risques associés à des mots de passe trop faibles, puis assurez-vous qu'ils soient améliorés
3. Limitez ou interdisez le Remote Desktop Protocol (RDP) à l'extérieur du réseau de l'entreprise ou activez Network Level Authentication
4. Utilisez un VPN lors de l'accès à distance
5. Contrôlez les réglages du pare-feu et fermez tous les ports non essentiels
6. Vérifiez les règles et politiques de trafic entre les systèmes internes de l'entreprise et les réseaux externes
7. Protégez à l'aide de mots de passe la configuration de vos solutions de sécurité
8. Segmentez le LAN de l'entreprise en sous-réseaux et connectez-les aux pare-feux pour limiter l'impact potentiel des attaques au sein du réseau
9. Préservez vos sauvegardes à l'aide de l'authentification multifacteur
10. Eduquez vos clients à reconnaître des cyberattaques et des ruses d'ingénierie sociale
11. Délimitez l'accès aux dossiers et documents partagés uniquement à ceux qui en ont besoin et restreignez autant que possible les contenus en lecture seule
12. Activez la détection des applications potentiellement dangereuses ou indésirables (PUSA/PUA)

3 Optez pour une solution de sécurité adaptée

Il est primordial d'intégrer à votre offre des fonctionnalités d'antivirus et de sécurité de périmètre, telles que le pare-feu ou l'antispam. Toutefois, en fonction des besoins de vos clients, de la verticale au sein de laquelle ils opèrent et des exigences réglementaires qui les concernent, une offre de produits additionnels tels que le chiffrement, l'authentification multifacteur ou la prévention de fuite de données (DLP), peut vraiment faire la différence.

Toutes ces solutions doivent **être faciles à déployer et à utiliser et ne pas nécessiter une maintenance trop importante**, ainsi votre expertise pourra être concentrée là où elle est vraiment nécessaire et permettre de gagner en fluidité pour votre client sans le déranger. Les solutions ESET sont conçues pour s'adapter à vos besoins (et ceux de vos clients) en travaillant sur la base "d'installer puis de passer à autre chose". Pour en tirer au mieux parti, voici quelques règles de base que les utilisateurs devraient respecter :

- **Utilisez la dernière version** de chaque produit
- **Gardez les fonctionnalités de sécurité** telles que ESET LiveGrid® et l'analyse en temps réel **activées.** Ces systèmes sont conçus pour collecter des informations sur les menaces et augmenter le niveau de protection des utilisateurs
- Si votre connexion internet le permet **mettez toujours à jour le moteur d'analyse et la base de données de détection** pour vous assurer que les points de terminaison gérés sont protégés contre les menaces nouvelles et émergentes
- **N'exécutez pas d'analyses manuellement :** cela consomme l'énergie de votre matériel tout en dupliquant inutilement l'activité de l'analyse en temps réel

Pour en savoir plus au sujet des services ESET pour les MSP, regardez ici.

ESET ne recommande pas aux utilisateurs d'exécuter eux-mêmes des analyses, sauf la première qui a lieu juste après l'installation. Ensuite, la protection en temps réel se charge de vérifier tous les nouveaux éléments que votre système peut rencontrer. Vous ne devriez lancer d'analyse que si votre protection en temps réel a été désactivée manuellement.

4

Eduquez vos clients et leurs utilisateurs

En tant que conseiller externe en sécurité, vous pouvez également créer de la valeur ajoutée auprès de vos clients en offrant à leurs employés une formation et une éducation à la cybersécurité. Il convient bien sûr d'adapter cet atelier à la connaissance et au niveau technique des employés à l'aide de plusieurs niveaux et selon la spécificité de chacun (management, personnel informatique, utilisateurs classiques...).

En fonction de la formation en cours, **les utilisateurs "classiques" sont aussi souvent décrits comme les plus vulnérables,** que cela concerne les techniques d'hameçonnage et d'ingénierie sociale, que d'autres formes de cyberattaques. Par conséquent, leur formation devra être la plus large possible, à commencer par ces conseils des plus basiques :

- Description des menaces les plus connues, telles que les malwares, l'ingénierie sociale et l'hameçonnage
- Des règles d'hygiène pour les mots de passe et l'importance de l'authentification multifacteur
- Meilleurs enseignements relatifs à la connexion aux réseaux
- Conseils et règles pour une navigation sécurisée
- Explication du spearphishing (hameçonnage ciblé), du whaling (chasse à la baleine ou encore fraude au président, en français) et des attaques ciblées - en particulier pour le top management et les employés qui sont en contact avec des contenus sensibles

Les MSP devraient également avoir un programme dédié pour l'équipe informatique de leurs clients, dans lequel des conseils et enseignements seraient expliqués afin de paramétrer au mieux les produits de sécurité ainsi que les réseaux et systèmes. A l'inverse des formations pour les utilisateurs finaux ou pour le top management, le programme destiné au personnel informatique devrait approfondir ses enseignements en détails techniques et couvrir un panel de sujets bien plus pointus :

- Des exigences minimales en matière de mots de passe, fréquence et configuration de la politique des mots de passe
- Une configuration correcte des profils administrateur et utilisateur dans le réseau de l'entreprise
- Des conseils pour minimiser la surface d'attaque des systèmes internes
- Des paramètres spécifiques pour des services officiels et légitimes qui sont détournés pour en faire des vecteurs d'attaques, tels que le remote desktop protocol (RDP), ou bien les emails et pièces jointes
- Des conseils détaillés sur la prévention aux ransomwares

ESET propose des contenus éducatifs, des guides et conseils destinés aux partenaires MSP et conçus pour être partagés avec vos clients.

5

Construisez une infrastructure adéquate et échangez avec votre client

La communication est essentielle, mais il vaut mieux miser sur la qualité que sur la quantité des échanges. En effet, vos clients attendent de vous que vous les informiez de manière compréhensible et complète sur l'état de leurs systèmes informatiques, mais seulement quand c'est vraiment nécessaire. Les solliciter de manière répétée au sujet d'événements mineurs peut vite devenir un réel fardeau pour votre client et le faire douter de vos compétences et de votre fiabilité.

Un partenaire MSP devrait avoir recours à des outils de sécurité adaptés fournissant des informations optimisées et une vue d'ensemble des anomalies détectées sur les endpoints ou sur d'autres espaces des systèmes qui méritent votre attention.

En cas d'incident de sécurité, une société MSP se doit d'être disponible et équipée, de manière **à agir vite** et à résoudre les problèmes potentiellement causés par l'incident en question. Si possible, la situation devrait pouvoir être gérée et résolue **à distance.** Pour atteindre cet objectif, une infrastructure correctement dimensionnée et **hautement résiliente,** de même qu'**une connectivité réseau fiable** sont indispensables.

En tant que MSP, vous devriez aussi être en mesure **de faire évoluer et d'ajuster vos systèmes**, car en effet, votre infrastructure ainsi que vos logiciels doivent constamment répondre aux besoins fluctuants de vos clients PME.

ESET propose une console robuste et mutualisée : ESET Security Management Center. Elle vous permet d'automatiser la résolution de problèmes de sécurité et de générer automatiquement des rapports avec votre logo, que vous pouvez ensuite faire suivre à vos clients. De plus, le système est facile à intégrer : nous prenons en charge une grande quantité d'outils RMM (Remote Monitoring and Management) et de consoles PSA.

6

Laissez tomber le modèle des “frais de service”, soyez un MSP moderne

Qu’on se le dise : la bonne vieille méthode de “frais de service” ou encore “panne/réparation” est clairement passée de mode dans le milieu des services de sécurité informatique.
Vos clients veulent en effet éviter les réparations trop chronophages et onéreuses qui ont souvent lieu sur le site de l’entreprise, ou avoir à leur charge la maintenance de leurs propres systèmes.

En tant que prestataire MSP moderne et à la page, voici ce que vous pouvez proposer à vos clients :

- **Des services à valeur ajoutée :** l’idée n’est plus à la vente de produits. Un MSP moderne se doit d’ajouter de la valeur à ses services et de persuader ses clients du bien-fondé de son expertise et de son expérience plutôt que de consacrer des ressources internes à ces activités.
- **Surveillance régulière de l’informatique sur site :** plutôt que de simplement installer puis de passer la main du contrôle de l’informatique et de la sécurité à son client, un MSP moderne doit proposer une surveillance continue et une maintenance des solutions fournies. Cela permet de réduire la charge du côté du client et de permettre au MSP de rester constamment informé de l’état et des changements des systèmes et réseaux du client.
- **Facturation ouverte et récurrente :** à l’instar de nombreux autres services en ligne, les MSP eux aussi adoptent un modèle de facturation ouverte et récurrente. Cela permet une plus grande souplesse et des solutions et services facilement déployés pour les clients.
- **Dialogues réguliers avec les clients :** en opposition au modèle précédent, les MSP d’aujourd’hui doivent impérativement communiquer et s’engager auprès de leurs clients régulièrement. Cela permet de créer des échanges plus personnalisés et d’éviter les malentendus.
- **Dépannage à distance :** un moyen pratique, moins long et par-dessus tout plus rapide pour résoudre des problèmes, comparé au modèle précédent qui nécessitait une intervention sur place.

Vos clients devraient toujours avoir un moyen simple de vous contacter. Pour vous assurer que ce soit toujours le cas, vous pouvez créer une série de fonds d’écran personnalisés dans lesquels se trouvent vos informations de contact. Ainsi, votre équipe sera toujours disponible pour vos clients en cas d’urgence informatique.


eset
CYBERSECURITY
EXPERTS ON YOUR SIDE